RON WYDEN
OREGON

RANKING MEMBER OF COMMITTEE ON FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5244

United States Senate
WASHINGTON, DC 20510-3703

COMMITTEES:
COMMITTEE ON FINANCE
COMMITTEE ON BUDGET
COMMITTEE ON ENERGY & NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

November 16, 2017

Rob Joyce
Cybersecurity Coordinator
The White House
1600 Pennsylvania Avenue Northwest
Washington, DC 20500

Dear Mr. Joyce:

I am writing to urge you to take prompt action to protect federal computer networks from cyberattacks perpetrated by foreign state actors and criminals by requiring agencies to block the delivery of malware-laden internet-based advertisements to their employees' work computers.

Malware is increasingly delivered through code embedded in seemingly innocuous advertisements online. Individuals do not even need to click on ads to get infected: this malicious software, including ransomware, is delivered without any interaction by the user. During the past few years, criminals have repeatedly delivered malware to American visitors to major news websites, social media, and streaming services by placing their malicious code in ads purchased through online advertising networks. Among other things, malware can steal, modify, or wipe sensitive government data, or remotely record conversations by remotely enabling a computer's built-in microphone.

According to recent media reports, Russia attempted to distribute malware-laden internet advertisements to at least one state election agency in August 2016. Although the vast majority of internet advertisements are legitimate, the fact that hostile actors can remotely target and potentially infect the computers of U.S. government employees means that this cyber threat vector can no longer be ignored. Using targeted ads, it is simply far too easy for foreign governments to deliver malicious code directly to the computers of government employees.

While the online advertising industry plays a vital role in the economics of the internet ecosystem, the threat posed by ad-delivered malware cannot be ignored. Indeed, several federal agencies have already recognized the serious nature of this cyber threat and, as a result, instituted network-based ad blocking. To that end, I ask that you do the following:

- Begin discussions with the online advertising industry and direct them to develop a plan within the next 180 days to ensure that online advertising networks cannot be used by foreign governments and criminals to deliver malware to U.S. government computers.

911 NE 11TH AVENUE
SUITE 630
PORTLAND, OR 97232
(503) 326-7525

405 EAST 8TH AVE
SUITE 2020
EUGENE, OR 97401
(541) 431-0229

SAC ANNEX BUILDING
105 FIR ST
SUITE 201
LA GRANDE, OR 97850
(541) 962-7691

U.S. COURTHOUSE
310 WEST 6TH ST
ROOM 118
MEDFORD, OR 97501
(541) 858-5122

THE JAMISON BUILDING
131 NW HAWTHORNE AVE
SUITE 107
BEND, OR 97701
(541) 330-9142

707 13TH ST, SE
SUITE 285
SALEM, OR 97301
(503) 589-4555

HTTP://WYDEN.SENATE.GOV

- After 180 days, if you are not completely confident that the advertising industry will effectively address this cyber threat, direct the Department of Homeland Security to issue a Binding Operational Directive requiring federal agencies to block the delivery to employees' computers of all internet ads containing executable computer code.

I appreciate your attention to this important matter. If you have any questions, please contact Chris Soghoian on my staff at (202) 224-5244.

Sincerely,

Ron Wyden
United States Senator

CC: Christopher Krebs, Assistant Secretary for Infrastructure Protection, Department of Homeland Security